CHAMBER OF DIGITAL COMMERCE

January 4, 2020
Via Federal E-Rulemaking Portal and
Via email: frc@fincen.gov

Policy Division
Financial Crimes Enforcement Network
P.O. Box 39
Vienna, VA 22183

Re: FinCEN Docket Number FINCEN-2020-0020, RIN 1506-AB47, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets"

To Whom it May Concern:

The Chamber of Digital Commerce (the "Chamber") welcomes the opportunity to submit this letter for consideration by the Financial Crimes Enforcement Network ("FinCEN") with respect to the Notice of Proposed Rulemaking regarding "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets" (the "NPRM").[1]

The Chamber is the world's largest blockchain trade association. Our mission is to promote the acceptance and use of digital assets and blockchain technology, and we are supported by a diverse membership that represents the blockchain industry globally. Through education, advocacy, and close coordination with policymakers, regulatory agencies, and industry across various jurisdictions, our goal is to develop a pro-growth legal environment that fosters innovation, job creation, and investment. We represent the world's leading innovators, operators, and investors in the blockchain ecosystem, including leading edge startups, software companies, global IT consultancies, financial institutions, insurance companies, law firms, and investment firms. Consequently, the Chamber and its members have a significant interest in blockchain and distributed ledger technology and the impact of the NPRM.

I. Introduction

The Chamber and its members support FinCEN's important goals of combatting money laundering, terrorist financing, and other illicit acts. Detecting and preventing bad actors from utilizing blockchain and distributed ledger technology is both the right thing to do and essential to the long-term growth and success of the industry. This commitment can be seen across the industry and our member base. For example, Chamber member blockchain analytics firms such as Chainalysis, Elliptic, CipherTrace, Netki, TRM Labs and others have developed cutting edge

[1] Requirements for Certain Transactions Involving Convertible Virtual Currency of Digital Assets, 85 Fed. Reg. 83,840 (Dec. 23, 2020) (hereinafter "NPRM").

compliance tools that provide insight and analysis into transactions beyond what is available in the traditional fiat world. Similarly, the Chamber itself is a co-founder of the Blockchain Alliance[2] and a co-lead in the Joint Working Group on the interVASP Messaging Standard to aid with global implementation of the funds travel rule and its recently released travel rule standard, IVMS 101.[3]

Notwithstanding its broad support for the Treasury Department's goals, the Chamber has a number of serious concerns with respect to the NPRM, many of which stem from the strikingly truncated process adopted by Treasury. The NPRM was not published in the Federal Register until December 23 giving commenters just 12 days over the Christmas and New Year's Day holidays to respond—which really amounts to a mere 6 business days (if you count Christmas Eve and New Year's Eve as business days) to comment. Such a limited period of time is wholly inconsistent with the potential impacts of this rule, as well as the recommendations of the Administrative Conference of the United States, which would generally provide at least 30 days for public comment on rulemakings (and 60 days for significant regulatory action as defined by Executive Order 12,866).[4]

To be clear, while we are submitting this comment letter within the prescribed period, it is impossible, within the limited period allowed, to provide a full response and analysis to the more than two dozen questions raised for public comment in the NPRM, and to address or even assess fully the broad range of issues and concerns raised by, and impact of, the proposed rule. In addition to the substantive comments provided below, we also address a number of open questions raised by various Chamber members which we have not been able to fully assess given the limited time provided to submit this comment letter. We have previously written to Secretary Mnuchin asking for a more careful and considered process, permitting 90 additional days to allow for more fulsome public comment, and we renew that request here.[5] We have also circulated a petition on Change.org, which, as of the time of this writing, has attracted over 5,000 signatures.[6]

Our concern with respect to this extraordinarily accelerated timetable is compounded by Treasury's assertion the proposed rule is exempt from the notice-and-comment requirements of the Administrative Procedure Act ("APA") and that "a longer period of public comment is not necessary and would frustrate the objectives of the rule by unduly delaying implementation of measures to curb illicit finance and threats to United States national interests." As discussed more fully below, it is impossible to reconcile Treasury's decision to apply notice-and-comment procedures, however inadequate, with its determination that notice-and-comment procedures would cause harm to the public interest and national security. Apart from this logical inconsistency

---

[2] BlockChain Alliance, https://www.blockchainalliance.org (last visited Jan. 4, 2020).
[3] interVASP Joint Working Group, interVASP Messaging Standard, https://intervasp.org/ (last visited Jan. 4, 2020).
[4] "Rulemaking Comments," Administrative Conference of the United States, June 16, 2011, Recommendation No. 2011-2, https://www.acus.gov/recommendation/rulemaking-comments.
[5] Press Release, Chamber of Digital Commerce, The Chamber of Digital Commerce Delivers Letter to U.S. Treasury Secretary Steven Mnuchin Urging Extension of NPRM Comment Period (Dec. 22, 2020), https://digitalchamber.org/letter-to-secretary-mnuchin/. *See also* Letter from Tom Emmer et. al., Members of Congress, to Steven T. Mnuchin, Sec'y of the Treasury (Dec. 31, 2020), https://emmer.house.gov/_cache/files/8/a/8a474348-cf14-467d-8c1d-bdc9c221df0a/7A3776731990BD312FCCE841E096D82B.congressional-letter-to-treasury-123120done.pdf.
[6] Chamber of Digital Commerce, *Extend the Comment Period! Sign Petition to Stop 11th Hour Treasury Rulemaking*, Change.org (last visited January 4, 2020), https://www.change.org/p/united-states-department-of-the-treasury-extend-the-comment-period-sign-petition-to-stop-11th-hour-treasury-rulemaking.

in the NPRM's APA analysis, the Chamber respectfully submits that a longer period of public comment is necessary given the complex nature of the topic and the broad impact of the rule. In addition, there is no evidence the objectives of the NPRM would be frustrated by providing additional time, and the NPRM does not qualify for any of the exceptions to default notice-and comment procedures.

In addition to these procedural concerns, the Chamber and its members have a number of concerns regarding the substance of the NPRM, including: (1) a misalignment between the purported goal of the rule and the rule's actual language and effect, (2) a severely understated estimation of the compliance burden placed on industry, (3) the likelihood the rule will undermine the important efforts of FinCEN to combat illegal use of cryptocurrencies by reducing the amount of actionable information reported and increasing the amount of unhelpful information reported, and (4) the likelihood that the rule will exacerbate existing privacy and cybersecurity considerations, and lead to a dramatic intrusion of government into the daily financial lives of Americans by providing Treasury visibility into nearly every blockchain transaction - past, present, and future - undertaken by banks' and MSBs' customers and the counterparties of those customers. We also offer a number of suggestions for clarifying and improving the rule as it is more fully considered.

Finally, we believe it is critical to note that self-hosted wallets play an important role in the digital asset ecosystem and, therefore, assertions that such wallets are inherently suspicious are unfounded. Self-hosted wallets are no different than the wallet in a consumer's handbag or pocket: they help consumers hold different tools and assets that are used in the digital world, just like a wallet holds a consumer's cash, credit cards, or driver's license and allows that consumer to spend cash whether at the coffee shop, the hardware store, or an online retailer. Indeed, self-hosted wallets can similarly be used for more than just convertible virtual currency ("CVC"), they can also be used to store a consumer's driver's license, professional degrees or licenses, and other non-currency related items, to provide just a couple of examples. Self-hosted wallets are also critical to the development of future innovations in the blockchain ecosystem, including efforts to create and spur the adoption of central bank digital currencies, currently under study by a number of central banks around the world including the Federal Reserve.

II. The NPRM Must Adhere to APA Notice and Comment Procedures

Given the significant impact of the proposed rule, the NPRM's 12-day/6 business day comment period is wholly inadequate and raises serious process concerns under the APA. Treasury is seeking to rush the rule to effectiveness where the only actual exigency is the change of Administration on January 20, 2021. While the comment period is nominally 12 days from publication of the NPRM in the Federal Register, that period includes Christmas and New Years' Day, federal holidays, as well as two weekends, effectively reducing the comment period to a mere 6 business days.[7] This does not comply with basic notions of due process or the plain letter of the APA, especially for a rule of this magnitude. As one court recently reasoned in invalidating a

[7] The NPRM also sites prior "engagements" between Treasury and industry on CVC-related matters including FinCEN Exchange events, visits to cryptocurrency businesses, and an industry roundtable with the Secretary. However, none of these events related to this particular NPRM and, instead, related to BSA matters generally. Therefore, the fact there were prior engagements between Treasury and industry on the BSA as a whole is irrelevant to whether industry had an opportunity to engage with Treasury on this specific rulemaking.

Department of Homeland Security rule adopted after providing an even longer 30-day comment period over a similar Christmas and New Years' holiday, "thirty days for a rule of this magnitude . . . is already short. That the comment period spanned the year-end holidays shortened the period further still and undercut the purpose of the notice process to invite broad public comment." *See Pangea Legal Servs. v. United States Dep't of Homeland Security*, No. 20-cv-07721, 2020 WL 6802474, *20 (N.D. Cal. Nov. 19, 2020).

The APA does not set a minimum period for comment, but courts have interpreted the APA to provide that an "exceedingly short" comment period does not "provide a meaningful opportunity for comment." *N. Carolina Growers' Ass'n, Inc. v. United Farm Workers*, 702 F.3d 755, 770 (4th Cir. 2012). Only in "rare" instances "actually warranting" a shortened comment period will a comment period as short as this one be permitted. Those rare situations "are generally characterized by the presence of exigent circumstances in which agency action was required in a mere matter of days." *Id.; see also Omnipoint Corp. v. F.C.C.*, 78 F.3d 620, 629 (D.C. Cir. 1996) (shortened comment period permissible where there was a "congressional mandate to implement the [rule] . . . 'without administrative or judicial delays'"). But the desire to rush a rule to effectiveness before the expiration of a presidential administration is not one of them.

The rush to make the Proposed Rule's regulations effective has placed an unsustainable burden on the industry, which has worked hard to provide what comments it can in the limited time allowed but could not possibly have addressed, or even evaluated, the many technical and legal issues that arise from the NPRM. One such example of the need to take further time arises from a recent, intervening statutory modification to FinCEN's authority to act.

At least as of the time of the NPRM's publication, serious questions arose regarding FinCEN's statutory authority to impose the NPRM's reporting and recordkeeping requirements on CVCs. Title 31 U.S.C. § 5313 permits the Secretary to require reporting of certain transactions "for the payment, receipt, or transfer of United States coins or currency (or other monetary instruments the Secretary of the Treasury prescribes." The NPRM declares that CVC is an "other monetary instrument." But the authority the Secretary invokes to define CVC as an "other monetary instrument" is limited to "coins and currency of a foreign country, travelers' checks, bearer negotiable instruments, bearer investment securities, bearer securities, stock on which title is passed on delivery, and similar *material*." 31 U.S.C. § 5312(a)(3) (emphasis added).

The NPRM does not address the meaning of the term "material" but, in the common understanding of the term, it denotes a *physical* substance or asset. *See, e.g.*, Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/material ("relating to, derived from, or consisting of matter," especially: PHYSICAL"); Webster's Third New International Dictionary ("the basic matter (as metal, wood, plastic, fiber) from which the whole or greater part of something physical (as a machine, tool, building, fabric) is made"). Indeed, each of the listed instruments is commonly represented in physical form (*e.g.*, bearer bonds, travelers' checks, stock certificates). The NPRM seeks to expand the statute's reach well beyond the world of physical assets, raising difficult questions of how this statutory authority translates into a digital environment in which some assets have no physical manifestation. These issues require much more careful vetting than the rushed process proposed by the NPRM.

Moreover, the recent passage of the National Defense Authorization Act for Fiscal Year 2021 ("NDAA") modifies the authorizing language contained 31 U.S.C. § 5321(a)(3) to include "value that substitutes for any monetary instrument" described in Section 5312(a)(3). However, the NDAA did not become law until January 1, 2021, when the Senate overrode the President's veto. With comments due the next business day, after the holiday weekend, it is simply impossible to fully evaluate the impact of this new NDAA language including whether CVC can and should be appropriately considered a monetary instrument under the new text and whether taking such an approach might have other unintended consequences or follow-on effects.

In light of this and similar challenges, the Chamber has done its best to provide what comments it could within the truncated comment period provided and has presented those issues of most immediate concern in this letter. However, there is much more that must be done, as evidenced by the list of open questions the Chamber has delineated in Section VII.

a. Good Cause Exception

While Treasury provides a (wholly inadequate) 12-day/6 business day period for comment, it also argues that the notice-and-comment requirements of the APA are entirely inapplicable. To this end, the agency asserts "good cause" under Section 553(d) as one of its justifications. That argument fails for several reasons.

First, the very fact that the agency has sought to comply with the notice-and-comment procedures fatally undermines its alternative claim that the "good cause" exception applies. The good cause exception requires that the agency explicitly find that notice-and-comment procedures themselves are "impracticable, unnecessary, or contrary to the public interest." 5 U.S.C. § 553(b)(B); *see also Mack Trucks, Inc. v. E.P.A.*, 682 F.3d 87, 93 (D.C. Cir. 2012). By publishing the proposed rule and providing for a comment period (albeit an inadequate comment period), the NPRM concedes that good cause is not present. Public comment cannot, by definition, be "impracticable" or "contrary to the public interest," where the agency has provided for public notice-and-comment.

In any event, there is no good cause to dispense with notice-and-comment in a rule of this magnitude. The exceptions provided in Section 553(b) "are not 'escape clauses' that may be arbitrarily utilized at the agency's whim." *Am. Fed'n of Gov't Emp., AFL-CIO v. Block*, 655 F.2d 1153, 1156 (D.C. Cir. 1981). The good cause exception "excuses notice and comment in emergency situations, or where delay could result in serious harm." *Jifry v. F.A.A.*, 370 F.3d 1174, 1179 (D.C. Cir. 2004) (citations omitted); *Block*, 655 F.2d at 1156 ("[U]se of these exceptions by administrative agencies should be limited to emergency situations."). Thus, "the good cause exception 'is to be narrowly construed and only reluctantly countenanced.'" *Mack Trucks*, 682 F.3d at 93.

That the agency here faces a self-imposed Inauguration Day deadline to act is not sufficient to support the good cause exception. "[D]eadlines in and of themselves do not generally provide a basis for invoking good cause on the ground of impracticability;" a "contrary rule would encourage administrative gamesmanship" and allow an agency to "wait until the eve of a statutory, judicial, or administrative deadline" and promulgate a rule without following the APA's procedures. *Mid Continent Nail Corp. v. United States*, 846 F.3d 1364, 1381 (Fed. Cir. 2017). This is especially

true of self-imposed, artificial deadlines for action. Courts regularly conclude that an "emergency of the [government's] own making" does not constitute good cause. *NRDC v. Abraham*, 355 F.3d 179, 205 (2d Cir. 2004); *compare, e.g., Levesque v. Block*, 723 F.2d 175, 184 (1st Cir.1983) (concluding imminence of self-imposed deadline did not qualify as good cause to dispense with notice-and-comment before issuing final rule); *with Council of the S. Mtns., Inc*. v. *Donovan*, 653 F.2d 573, 581 (D.C.Cir.1981) (noting, among other things, that circumstances creating exigency "were beyond the agency's control").

The circumstances here do not satisfy any of the statutory standards for good cause. The NPRM does not identify emergency circumstances sufficient to satisfy the impracticability standard. *See Util. Solid Waste Activities Grp. v. E.P.A.*, 236 F.3d 749, 754 (D.C. Cir. 2001) ("impracticability" applies when a statute would "pose[] any threat to the environment or human health" without amendment or if "some sort of emergency had arisen"). The exigency identified by Treasury—avoiding the opportunity for bad actors to hide assets during the consideration of the rule—is fatally undermined by its allowance of *any* advanced notice of action. Withdrawals from cryptocurrency platforms take place in a matter of minutes or hours, not weeks. It is therefore difficult to see how an additional 30, 60, or 90 days would have a material impact on this concern. (In this case, we note that Treasury even published the unofficial version of the proposed rule on its website 5 days prior to the official publication in the Federal Register, thus "tipping off" would be bad actors, if they were to act on advanced notice.)

Perhaps more importantly, there is little evidence that this NPRM in itself will cause a rush of bad actors off CVC platforms. Banks and MSBs are already required to file SARs and to comply with other recordkeeping requirements contained in the Bank Secrecy Act ("BSA") and implemented by FinCEN regulations. Banks are also already subject to a customer identification program ("CIP") rule and customer due diligence ("CDD") rule and MSBs are already subject to a number of rules and recordkeeping requirements that mandate knowing their customers by collecting and retaining information.[8] FinCEN recently published other rules, such as the Funds Transfer/Travel Rule NPRM giving public notice (and a slightly more expansive, albeit still far too short, 30-day opportunity for public comment) of its intent to enhance recordkeeping requirements applicable to convertible virtual currency platforms.

Similarly, the agency cannot credibly conclude that notice and comment is "unnecessary," as that exception is "confined to those situations in which the administrative rule is a routine determination, insignificant in nature and impact, and inconsequential to the industry and to the public." *See Mack Trucks*, 682 F.3d at 94; *see also* Attorney General's Manual on the Administrative Procedure Act (1947) at 31 ("'Unnecessary' refers to the issuance of a minor rule or amendment in which the public is not particularly interested."). There is nothing routine about the substantial and costly new reporting and recordkeeping requirements for transactions involving self-hosted wallets addressed in the NPRM – impacts FinCEN itself has acknowledged in the NPRM.

Nor is it in the public interest to dispense with notice-and-comment, as the agency effectively admits in permitting *some* (but insufficient) time for public comment. The "public interest" exception "is met only in the rare circumstance when ordinary procedures—generally presumed

[8] *See* 31 C.F.R. Part 1020 for banks and Part 1022 for MSBs.

to serve the public interest—would in fact harm that interest." *Mack Trucks*, 682 F.3d at 95; *See also* Attorney General's Manual at 31. ("The question is not whether dispensing with notice and comment would be contrary to the public interest, but whether providing notice and comment would be contrary to the public interest."). *See also* Attorney General's Manual on the Administrative Procedure Act at 30 ("'Public interest' connotes a situation in which the interest of the public would be defeated by any requirement of advance notice."). The public interest is served by regular notice-and-comment procedures for a rule of such far reaching impact as this one.

For similar reasons to those stated above, the agency should not seek to invoke good cause to eliminate the 30-day post-publication requirement of 5 U.S.C. § 553(d). In order to invoke "good cause" to waive the 30-day delayed effective date of Section 553(d), the agency must make a separate good cause determination. *See, e.g., United States v. Brewer*, 766 F.3d 884, 888 (8th Cir. 2014) ("courts should not conflate the pre-adoption notice-and-comment requirements, listed in § 553(b) and (c), with the post-adoption publication requirements, listed in § 553(d). Because these are separate requirements, the agency must have good cause to waive each."); *Conyers v. Sec'y of Veterans Affairs*, 750 F. App'x 993, 999 (Fed. Cir. 2018).

A separate "good cause" argument to waive the 30-day delayed effective date for this NPRM would similarly fail. Especially here, where compliance will require new and complex measures to identify and report affected transactions, regulated companies should have sufficient time to prepare for compliance. The agencies' stated justification for arguing that notice-and-comment rules need not apply to the new regulations—avoiding transmitting the content of the rule to bad actors and preventing pre-publication circumvention of the rules' obligations—does not hold water with respect to the comment period, as described above, and is even less applicable to the pre-publication period given the passage of time. At the very minimum, the agency should permit the full 30-day effective date period required by Section 553(d),[9] and as described more fully below, should implement a delayed compliance date to accommodate the anticipated cost and technical preparations needed to comply.

b. Foreign Affairs Function Exception

For similar reasons, the agency's invocation of national security does not satisfy the "foreign affairs function" exception to 5 U.S.C. § 553. "The foreign affairs exception, like all similar exceptions to the APA's notice-and-comment requirements, is quite narrow." *Invenergy Renewables LLC v. United States*, 422 F. Supp. 3d 1255, 1289 (Ct. Int'l Trade 2019). The phrase "foreign affairs function" should not be interpreted loosely "to mean any function extending beyond the borders of the United States." *City of New York v. Permanent Mission of India to United Nations*, 618 F.3d 172, 202 (2d Cir. 2010). As Congress noted in considering the APA, the foreign affairs function exception reaches "only those 'affairs' which so affect relations with other governments that, for example, public rule making provisions would clearly provoke definitely undesirable international consequences." S. Rep. No. 752, 79th Cong., 1st Sess. 13 (1945) (emphasis added). Thus, the government must demonstrate that the rule at issue "clearly and directly" involves "activities or actions characteristic to the conduct of international relations." *Capital Area Immigrants' Rights Coalition v. Trump*, 471 F. Supp. 3d 25, 53 (D.D.C. 2020).

[9] We reiterate that the Chamber has asked for 90 days in which to comment. *See* Chamber letter to Secretary Mnuchin, supra note 5.

The foreign affairs function exception plainly does not apply here. The rule does not clearly and directly implicate the activities and actions characteristic of foreign relations—this is a financial disclosure and recordkeeping rule primarily applicable to domestic transactions (transactions involving foreign financial institutions are specifically exempted from the rule's applicability, with certain exceptions). Any incidental and indirect effects on foreign states or actors is insufficient to support the foreign affairs exception. *See Capital Area Immigrants' Rights Coalition,* 471 F. Supp. At 55-56.

Moreover, the arguments Treasury now makes for foregoing meaningful notice and comment based on the foreign affairs function exception could be made for every rule implemented under the Bank Secrecy Act. If one were to adopt Treasury's arguments, Treasury should never have to seek notice and comment from industry for any proposed rule under the BSA because, according to Treasury, it involves a foreign affairs function with cross border implications designed to prevent money laundering and terrorist financing. However, this would be contrary to Congress's express design, since Congress had the opportunity to, but did not, exempt the BSA entirely from the requirements of the APA simply because it had implications beyond our borders. Moreover, this has certainly not been the practice of FinCEN in regulating under the BSA. *See* Examples Cited, *infra*.

To deprive the American public of the right to comment on such important regulations, the government must do more than simply tie, however indirect and attenuated, to international affairs. *See E. Bay Sanctuary Covenant v. Trump,* 932 F.3d 742, 775 (9th Cir. 2018) (foreign affairs function exception "requires the Government to do more than merely recite that the Rule 'implicates' foreign affairs"). It is not merely the subject matter of the rule that matters, but whether proceeding with ordinary notice and comment requirements would "provoke definitely undesirable international consequences.'" *Am. Ass'n of Exporters & Importers-Textile & Apparel Grp. v. United States*, 751 F.2d 1239, 1249 (Fed. Cir. 1985) (quoting H. Rep. No. 1980, 69th Cong., 2d Sess. 23 (1946)); *Rajah v. Mukasey*, 544 F.3d 427, 437 (2d Cir. 2008) ("For the exception to apply, the public rulemaking provisions should provoke definitely undesirable international consequences."). Courts "have disapproved the use of the foreign affairs exception where the Government has failed to offer evidence of consequences that would result from compliance with the APA's procedural requirements." *Id*. at 776.

There is no evidence here that compliance with the APA's notice-and-comment procedures would do any harm to the U.S. international relations. FinCEN's determination to apply notice-and-comment procedures fatally undermines any claim that such procedures would "provoke definitely undesirable international consequences." *Rajah*, 544 F.3d at 437. The proposed rule concludes that notice-and-comment is not necessary because the proposal seeks to establish controls to protect the national security "from a variety of threats from foreign nations and foreign actors," but these concerns alone do not demonstrate that an appropriate public comment period would provoke "undesirable international consequences." Indeed, all of the categories of illicit conduct cited in the NPRM (such as "state-sponsored ransomware and cybersecurity attacks, sanctions evasion, and financing of global terrorism, among others") have unfortunately been ongoing for years. The NPRM presents no evidence or even allegations of new developments that have suddenly made years-long concerns a matter of urgency and, in fact, highlights the long-known nature of such concerns in the footnotes it uses for support, which cite examples going back to

2017 for support of exigent circumstances.[10] If such conduct did not require urgent regulatory action in 2017, it certainly doesn't necessitate the present severely abbreviated rulemaking process.

The NPRM's citation of the threat that "undue delay" in implementation "would encourage movement of unreported and unrecorded assets in illicit finance" during a lengthier comment period is without merit for the reasons outlined above with respect to the "good cause" exception. Extending that period to allow appropriate input will not cause any significant additional harm, since suspicious actors and funds transfers are already well-covered by existing BSA regulations applicable to banks and MSBs, and this type of normal notice-and-comment period will permit the agency to have the full benefit of the input of the blockchain industry and other affected parties, including law enforcement. This rule is complex in application – rushing it through will only harm law enforcement efforts, not aid them.

Finally, FinCEN has not sought to avoid the APA's notice-and-comment provisions for similar past rulemakings. Consider, for example:

- "Threshold for the Requirement To Collect, Retain, and Transmit Information on Funds Transfers and Transmittals of Funds" – 30-day comment period;[11]
- "Customer Identification Programs, Anti-Money Laundering Programs, and Beneficial Ownership Requirements for Banks Lacking a Federal Functional Regulator" – 60-day comment period;[12]
- "Proposal of Special Measure Against Bank of Dandong as a Financial Institution of Primary Money Laundering Concern" – 60-day comment period;[13]
- "Imposition of Special Measure Against North Korea as a Jurisdiction of Primary Money Laundering Concern" – 60-day comment period;[14]
- "Amendment to the Bank Secrecy Act Regulations; Defining Mutual Funds as Financial Institutions" – 90-day comment period;[15] and
- "Customer Due Diligence Requirements for Financial Institutions" – 60-day comment period.[16]

---

[10] NPRM at footnote 2.
[11] Threshold for the Requirement To Collect, Retain, and Transmit Information on Funds Transfers and Transmittals of Funds Transfers That Begin or End Outside the United States, 85 Fed. Reg. 68005 (Oct. 27, 2020).
[12] Customer Identification Programs, Anti-Money Laundering Programs, and Beneficial Ownership Requirements for Banks Lacking a Federal Functional Regulator, 81 Fed. Reg. 58425 (Aug. 25, 2016).
[13] Proposal of Special Measure Against Bank of Dandong as a Financial Institution of Primary Money Laundering Concern, 82 Fed. Reg. 31537 (July 7, 2017).
[14] Imposition of Special Measure Against North Korea as a Jurisdiction of Primary Money Laundering Concern, 81 Fed. Reg. 35665 (June 3, 2016).
[15] Defining Mutual Funds as Financial Institutions, 74 Fed. Reg. 26996 (proposed June 5, 2009).
[16] Customer Due Diligence Requirements for Financial Institutions, 79 Fed. Reg. 45151 (Aug. 4, 2014). We note that, while this particular NPRM had a 60-day comment period, issuance of a final CDD rule was in fact a multi-year process. The Customer Due Diligence requirement, imposing on banks certain recordkeeping obligations regarding beneficial ownership of corporate customers, was initiated through an Advanced Notice of Proposed Rulemaking in March 2012 and concluded with a Final Rule in May 2016 – over four years of industry consultation and feedback on the specific requirements of the rule. *See* Customer Due Diligence Requirements for Financial Institutions, 77 Fed. Reg. 13046 (Mar. 5, 2012); Customer Due Diligence Requirements for Financial Institutions, 79 Fed. Reg. 45151 (Aug. 4, 2014); Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. 29398 (May 11, 2016).

It is difficult to see how the current NPRM addresses a situation more exigent than any of the other NPRMs listed above. The above NPRMs similarly relate to matters of customer verification, recordkeeping, and reporting. FinCEN did not determine that a 30, 60, or 90-day comment period would undermine the effectiveness of these rules and the current NPRM provides no explanation – nor could it – for why its requirements are different from those contained in the above.

III. The NPRM Will Reduce the Reporting of Useful Information and Increase the Reporting of Unhelpful Information

The Chamber strongly supports efforts to prevent and identify money laundering, terrorist financing, and other bad acts, including regulatory changes that are likely to result in a reduction in illicit finance. However, we believe the NPRM may have the opposite effect, undermining those critical goals by reducing the reporting of helpful information and increasing the reporting of unhelpful information.

The NPRM notes that FinCEN "received approximately $119 billion in suspicious activity reporting associated with CVC activity taking place wholly or in substantial part in the United States"[17] and FinCEN officials regularly cite the importance of SARs as a critical law enforcement tool. As recently stated by FinCEN Director Kenneth Blanco:

> *Since 2013, FinCEN has received nearly 70,000 Suspicious Activity Reports (SARs) involving virtual currency exploitation. Just over half of these reports come from virtual currency industry filers, likely many of you participating today .... This reporting is incredibly valuable to FinCEN and law enforcement, especially when you include technical indicators associated with the illicit activity, such as Internet Protocol (IP) addresses, malware hashes, malicious domains, and virtual currency addresses associated with ransomware or other illicit transactions.*[18]

Unfortunately, this NPRM, which targets hosted-to-self-hosted wallet transactions, is just as likely to reduce SAR reporting by incentivizing BSA-regulated entities to engage in de-risking and raising the burdens placed on consumers when dealing with such entities, thereby pushing transactions toward entirely self-hosted, peer-to-peer ("P2P") dealings with no involvement from BSA-regulated entities.

To offer just one example, consider ransomware payments. Where a victim of a ransomware attack makes a payment through a BSA-regulated entity, that entity will obtain and retain significant details regarding the transactions, potentially including blockchain analytics, and will likely file a SAR. However, under the NPRM, in order to process such a payment, the victim would need to provide the name and physical address of its counterparty (the recipient), which it will typically be unable to do. Victims will then be left with only the option of making the payment in a P2P fashion without the involvement of any BSA-regulated entity, resulting in a potential loss of

[17] NPRM at 83842.
[18] FinCEN, Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered at the Consensus Blockchain Conference (May 13, 2020), https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-consensus-blockchain.

critical data for law enforcement. Indeed, FinCEN's recent guidance regarding ransomware included a section dedicated to SAR filing with special instructions for filing ransomware-related SARs, indicating the agency finds such reports valuable.[19]

On the other hand, the NPRM will result in the filing of a voluminous amount of CVC transaction reports. One of our members has estimated it would be required to file approximately 39,000 CVC transaction reports a year. Unlike in the CTR context, where there are limited reasons to be handling $10,000 or more in physical cash, transactions involving self-hosted wallets over $10,000 occur all the time for a variety of legitimate reasons such as paying for goods and services, paying employee salaries, and making investments, to name just a few. Many transactions above that threshold are also likely to include customers transferring CVC to their own self-hosted wallets if, for example, they no longer wish to hold their assets at a given bank or MSB to reduce counterparty risk or for security reasons, for example. Therefore, the significant majority of CVC transaction reports filed are likely to be of no law enforcement value.

The NPRM thus will reduce the reporting of useful information, in the form of SARs, and increase the reporting of largely unhelpful information in the form of CVC transaction reports. The Chamber believes such a result is the opposite of what law enforcement would want and encourages the Treasury Department to engage in further dialogue with law enforcement agencies on this topic.

Importantly, we note that the NPRM, which takes a one size fits all approach to transactions involving self-hosted wallets, cuts against other recent FinCEN actions intended to "provide financial institutions greater flexibility in the allocation of resources and greater alignment of priorities across industry and government, resulting in the enhanced effectiveness and efficiency of anti-money laundering (AML) programs."[20] Viewing all self-hosted wallet transactions as inherently suspicious will prevent banks and MSBs from focusing compliance resources on activity that is the most likely to present money laundering and related risks and cuts against the risk-based approach that FinCEN generally advocates.[21] Such an approach also undermines recent actions from other governmental agencies, such as the Office of the Comptroller of the Currency, which recently issued a proposed rule that, if implemented, would prohibit national banks and federal savings associations from categorically declining to service industries engaged in lawful business activities.[22] Rather, the OCC's proposed rule would require covered institutions to conduct a risk-based assessment of each customer before making a decision whether to provide services.[23]

---

[19] FinCEN, Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments (Oct. 1, 2020), https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf.

[20] FinCEN, FinCEN Seeks Comments on Enhancing the Effectiveness of Anti-Money Laundering Programs (Sept. 16, 2020).

[21] *See, e.g.,* FinCEN, Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States (Apr. 26, 2005), https://www.fincen.gov/sites/default/files/guidance/guidance04262005.pdf; Financial Action Task Force, FATF takes action to tackle de-risking (Oct. 23, 2015), https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-action-to-tackle-de-risking.html.

[22] Fair Access to Financial Services, 85 Fed. Reg. 75261 (Nov. 25, 2020).

[23] *Id.*

From a risk-based perspective, there is reason to believe that self-hosted-to-hosted transactions (and vice versa) are among the safest in the blockchain ecosystem. Transactions taking place entirely within hosted environments, such as custodial exchanges, generally involve off-chain transfers, meaning traditional blockchain analytics tools are not applicable. Conversely, transactions taking place in an entirely self-hosted environment lack the involvement of a BSA-regulated entity, which typically maintain robust know your customer ("KYC") and monitoring procedures. Transactions in the self-hosted-to-hosted context allow for use of blockchain analytics tools and the compliance resources of BSA-regulated entities, making them highly desirable transactions to encourage (rather than discourage) in the blockchain ecosystem.

Analysis from Chainalysis, a leading blockchain analytics provider widely relied upon by regulators, law enforcement, and industry alike, indicates that 92% of bitcoin transactions between self-hosted wallets in the second quarter of 2020 originated from digital asset exchanges or other regulated financial institutions.[24] This analysis further supports the above arguments that the NPRM would primarily capture lower-risk transactions where law enforcement already has substantial insight and would generate a massive volume of reports with no law enforcement value. Similarly, Chainalysis assesses that a significant majority of bitcoin moving between self-hosted wallets is eventually received by a regulated financial institution, meaning there is law enforcement insight on both ends of the transaction chain.[25] As explained by Chainalysis, "The vast majority of bitcoin both sent and received by unhosted wallets has an exchange in a regulated environment as the counterparty, with the resources to help law enforcement."[26] Finally, the report notes that 30% of bitcoin held in self-hosted wallets moves just once per month and the frequency of "USD M2 money" transactions is 4.7 times higher than that of bitcoin, further undermining the notion that self-hosted wallets present a unique law enforcement challenge. Therefore, we believe it is clear the NPRM is significantly overbroad in its application and is likely to be detrimental, rather than helpful, to law enforcement.

Importantly, while entirely self-hosted, P2P transactions may offer law enforcement somewhat less insight than compared to hosted-to-self-hosted transactions, the Chamber does not believe that P2P transactions are inherently risky and note that such transactions are almost certainly less risky than transactions conducted in physical currency. As noted above, self-hosted wallet transactions are traceable on the blockchain, typically involve one or more BSA-regulated financial institutions at some point in the payment chain (*e.g.*, fiat on- and off-ramps), and are conducted at a lesser frequency than transactions in fiat-denominated money. Therefore, while hosted-to-self-hosted transactions are among the safest transactions anywhere in the financial system, any attempt to cast transactions entirely between self-hosted wallets as inherently risky is inaccurate and clearly contrary to existing evidence, and may draw attention away from potentially riskier transactions already reported to FinCEN using the SAR process.

[24] *What You Need to Know About Treasury's 72-page NPRM for Transactions with Unhosted Wallets and Certain Foreign Jurisdictions,* Chainalysis Blog (Dec. 22, 2020), https://blog.chainalysis.com/reports/treasury-department-nprm-unhosted-wallets-2020.
[25] *Id.*
[26] *Id.*

Finally, given the ability to trace even self-hosted to self-hosted wallet transactions using blockchain analytics and other risk mitigation measures described above, it is inappropriate and potentially harmful to treat CVC transactions as riskier than currency transactions by applying more stringent verification and reporting requirements in the CVC context as compared to the current CTR rule. Such an approach risks distracting attention away from riskier currency transactions based on the need to process and analyze the much greater amount of information that would be required by the NPRM for CVC transactions.

IV. The NPRM Underestimates the Burden Placed on Industry and Ignores Significant Challenges

a. The Burden Analysis Contained in the Rule is Fundamentally Flawed

The NPRM concludes that the total annual burden hours imposed by the proposed rule would amount to 1,284,349 hours.[27] While imposing over a million burden hours on an emerging industry would in itself be a significant cost on the industry, undermining its ability to innovate and compete with rival offerings, including those from adversarial countries such as China and many others, the Chamber believes the NPRM significantly underestimates the true burden that would be imposed by the proposed rule. Indeed, the calculation provided in the NPRM relies on a number of false assumptions that render the analysis wholly inadequate.

First, in conducting the burden hour analysis for both the recordkeeping and reporting requirement, the NPRM "assumes" that the burden in the Funds Transfer/Travel Rule NPRM context is "analogous" to the burden imposed by the current NPRM and uses the Funds Transfer/Travel Rule NPRM estimate as the basis for analysis in the current NPRM, making adjustments for certain differences between the proposed rules.[28] This approach is fundamentally flawed as it assumes, without justification, that the burden estimate contained in the Funds Transfer/Travel Rule NPRM is accurate. In fact, a number of the public comments submitted in response to the Funds Transfer/Travel Rule NPRM pointed to flaws in the burden hour estimate contained in that rule.[29] A final rule, responding to public comments and addressing the burden-hour estimate set forth in that NPRM, has not yet been issued. Therefore, the current NPRM bases its burden estimate on an analogy to a faulty estimate contained in another proposed rule, about which industry has already raised concerns and to which FinCEN has not yet responded.

Second, the burden hour analysis in the NPRM is significantly flawed with respect to the total number of transactions that would be covered by the proposed reporting and recordkeeping provisions. Both provisions contain exceptions for "a transaction in convertible virtual currency or a digital asset with legal tender status that is between the financial institution's customer and a counterparty whose account is held at a financial institution regulated under the BSA, or at a foreign financial institution" with the exception of foreign financial institutions located in certain

[27] NPRM at 83854.
[28] NPRM at 83857.
[29] *See e.g.*, Letter from Andreessen Horowitz, Paradigm, & Union Square Ventures, the Commenters, to Ann E. Misback, Sec'y of the Bd. of Governors of the Fed. Rsrv. Sys. (Nov. 27, 2020) at Section V., https://www.regulations.gov/document?D=FINCEN-2020-0002-2825.

jurisdictions.[30] In estimating the burden hours required to comply with the proposed rule, the NPRM wrongly assumes that banks and MSBs will always know when a transaction involves another hosted wallet at a BSA-regulated entity or foreign financial institution and therefore uses only transactions between hosted and self-hosted wallets when conducting its analysis. In fact, given the difficulty industry has in knowing this data, it is hard to understand how Treasury purports to estimate this figure.

In reality, it is likely that banks and MSBs will not know whether another wallet is a hosted or self-hosted wallet for a significant number of transactions – for example, a customer may not know the institution holding the wallet of their counterparty. Even if a customer was able to provide a bank or MSB with the name of an institution, it will not always be possible to determine if that entity is a BSA-regulated entity or foreign financial institution. For example, while FinCEN has a public database of MSB registrants, many companies operate under a trade name or have multiple operating entities, only one of which is registered with FinCEN (because the other entities are not engaged in money transmission or because they do not operate in the United States). In addition, even if a bank or MSB knew a given entity was a BSA-regulated financial institution or a foreign financial institution, it is not always possible to know with certainty that a given wallet address is in fact held at that entity.[31] Therefore, banks and MSBs will inevitably record and report on a significant number of transactions that involve hosted wallets only and that are not included in FinCEN's analysis.

Third, the NPRM states that the burden analysis was conducted by a review of data related to "two major exchanges in September 2020." The NPRM does not state which exchanges were reviewed, and there is no reason to believe that two randomly selected "major" exchanges are reflective of the industry at large.

Fourth, the NPRM lacks several critical pieces of data necessary to determine the likely burden imposed by the proposed rule even if sufficient time were provided. For example, the NPRM does not provide a draft of the form that industry will use to report CVC transactions and, instead, states, "Such report shall include, in a form prescribed by the Secretary, the name and address of each counterparty, and such other information as the Secretary may require."[32] The lack of a draft form and ability for the Secretary to require the reporting of additional information not described in this NPRM as part of the form means there is no manner to accurately estimate the burden imposed by the NPRM. (Nor do we believe that providing the Secretary such substantial discretion to alter the reporting requirement without seeking industry input is warranted or appropriate.) Similarly, while the Chamber assumes that FinCEN will permit batch reporting of CVC transactions, such batch reporting is not explicitly called for in the NPRM and the absence of a batch reporting mechanism would dramatically impact the burden on industry.

[30] NPRM at 83860 and 83861.
[31] While blockchain industry firms are developing tools that, if widely adopted across industry, would help in identifying hosted wallet providers, such tools are not yet implemented at scale.
[32] NPRM at 38360.

b. Overarching Implementation Challenges Not Addressed in the NPRM

In addition to the flaws in the burden analysis, the analysis does not consider a number of important factors that not only further demonstrate the inadequacy of the burden analysis contained in the NPRM, but also highlight the significant implementation hurdles faced by industry. Overcoming these hurdles is likely to be extremely costly, perhaps prohibitively so for many members of industry. More importantly, even if banks and MSBs subject to the NPRM had unlimited compliance resources, in many instances, achieving full compliance may not be possible in the absence of significant de-risking and/or overreporting. We highlight below a few of the implementation challenges that have been most commonly cited by our members and apply to the industry as a whole. Other potential implementation challenges, particularly those arising from the vague and incomprehensive nature of the NPRM, that may apply depending on a member's given business model, are included below in Section VII where we address additional questions raised by the NPRM.

1. Technology to implement aggregation and structuring detection

First, the NPRM states that "multiple convertible virtual currency … transactions shall be treated as a single transaction if the bank or money services business has knowledge that they are by or on behalf of any person and result in value in or value out of convertible virtual currency … with a value of more than $10,000 during a 24-hour period."[33] This means that banks and MSBs will need to implement new technology solutions to aggregate transactions, including transactions conducted in different CVCs, and to do so on a continuous, rolling 24-hour basis.[34] Implementing a technology solution of that nature is a costly and time-intensive endeavor that even the most sophisticated financial institutions will have difficulty doing in such a short timeframe. While some banks and MSBs already have CVC transaction monitoring tools in place, such tools are not currently calibrated to identify aggregation or structuring activity specific to this NPRM and would need to be updated and expanded as a result. Banks and MSBs will also need to develop similar technology solutions to detect structuring around the new reporting requirement, another costly and time intensive undertaking.

2. Accurately identifying hosted wallets

Second, as noted above, in many cases, banks and MSBs will have difficulty determining whether a counterparty wallet is held by a BSA-regulated entity. Banks and MSBs will have to spend considerable compliance resources, both in terms of technology and human capital, to review counterparty wallet addresses and, even after a rigorous review, may not be able to make a determination with respect to the status of a counterparty's wallet. One member predicts spending $150,000-$200,000 a year on this activity alone and notes that, for certain blockchain protocols, it will likely to be impossible to make any determinations given the lack of available technological tools at present. As a result, affected financial institutions have indicated that they may need to

[33] NPRM at 38360.

[34] The Chamber also notes that aggregation across CVCs is unnecessary and not in keeping with Treasury's practice in other contexts (*i.e.,* currency movements are not aggregated with ACH movements). To the degree aggregation is required it should be limited to aggregation within specific CVCs.

treat all counterparties as self-hosted wallets for both the recordkeeping and reporting obligations, which will inevitably lead to significant over-reporting of CVC transactions.

3. Obtaining counterparty information on incoming transfers

Third, the NPRM places banks and MSBs in an impossible bind by requiring the retention of counterparty information for all inbound transactions over $3,000, even those for which it receives no prior notice and has no control over the sender. The NPRM seemingly recognizes that banks and MSBs cannot prevent third parties from sending CVC to wallets that they host by allowing such entities to obtain the required recordkeeping and verification information "as soon as practicable." However, it ignores the likelihood that, at least in some situations, a bank or MSB will receive a CVC transaction with no prior notice and be unable to subsequently conduct the recordkeeping and verification requirements. The inability to collect such information could arise in a number of situations such as: (1) the bank or MSB's customer declines to provide the necessary information, (2) the bank or MSB's customer doesn't know the name or physical address of the transmitter, or (3) CVC is received from a smart contract or similar decentralized application that lacks a single identifiable owner (such as protocols jointly owned by hundreds or thousands of individuals holding governance tokens). In such situations, banks and MSBs could be penalized for non-compliance even though such entities have no control over the situation and could not reasonably be expected to have prevented such an outcome.

These are just a few of the significant hurdles facing industry making compliance with the NPRM extremely costly and, at least in some instances, impossible absent significant de-risking and/or overreporting. As noted, other implementation challenges that may apply depending on a member's specific business model are included below in Section VII.

c. Impact on Our Members

Even in the short amount of time provided for comment, we have received quantified impact estimates from a number of members expressing significant concern regarding the compliance burdens that would be imposed by the proposed rule. One member indicated it would likely need to hire two additional full-time staff focused exclusively on compliance with this rule. Another member estimated the compliance cost as between $250,000-$500,000 a year and estimated it would be required to file approximately 39,000 reports a year, and yet another estimated it would be required to file 52,000 CVC transaction reports annually and that the cost of compliance would be double the per-MSB burden hours predicted by Treasury in the NPRM even before taking into account any costs related to the creation and maintenance of technology solutions, which are likely to be substantial.

Multiple members have expressed significant concern over the cost of developing technology solutions to comply with the aggregation and structuring requirements (discussed above) and questioned whether it would be possible to develop a solution in time to comply with a final rule. For example, one member's preliminary estimate of the cost of developing necessary technology solutions was between $500,000 and $1,000,000.

Members have also cited a wide variety of categories in which additional costs are likely to arise, and which are not specifically addressed in the NPRM, including:

- Audit Costs: the cost of required independent compliance program audits would increase given the expanding nature of the regulatory requirements addressed by such programs;
- Counsel Costs: members anticipate external counsel costs associated with interpretation of the regulation with respect to their specific business models;
- Vendor Costs: vendor costs related to identification of hosted wallets will likely be significant. Given the likely volume of covered transactions, members anticipate the need to hire vendors to provide compliance-related software and services. Along with securing said vendors, members anticipate having to allocate vendor management and due diligence resources to properly evaluate potential vendors;
- Record Retention: members anticipate retaining records related to identification of hosted wallets, evidence of due diligence on potential hosted wallets, records of CVC transaction reports, and corresponding supporting documentation, among other records. Costs related to storage will likely rise due to an increase in volume of compliance records that must be retained for five years, in order to comply with the new regulation; and
- Technology Costs: members anticipate making system enhancements in order to:
    - Flag transactions meeting the $3,000 recordkeeping and $10,000 reporting requirements;
    - Aggregate transactions by each covered wallet across multiple digital assets, multiple customer accounts, and multiple platforms or branches with which a customer may establish a relationship;
    - Identify potential structuring activity by customers seeking to evade recordkeeping and reporting thresholds, especially given the requirement is based on a rolling 24-hour basis as opposed to a calendar day;
    - Develop other technology solutions to enhance or automate processes currently done manually given the significant increase in compliance responsibilities contemplated by the NPRM;
    - Enhancements to screening tools to identify when FinCEN makes changes to the Foreign Jurisdictions List; and
    - Compile and upload CVC transaction reports (assuming batch reporting is permitted).

These are just a few of the examples that have been provided to the Chamber by its members, and which themselves represent but a fraction of the quantification that could be done during a normal comment period. They nevertheless highlight the significant burden the NPRM would impose on industry and further support the notion that the burden estimate contained in the NPRM does not accurately capture the true cost of compliance.

d. Additional Compliance Challenges Raised by Specific Questions in the NPRM

In addition to the compliance challenges cited above, the Chamber was concerned by a number of specific questions contained in the NPRM that suggest a potential desire on the part of Treasury to expand the recordkeeping and reporting requirements beyond what is currently contained in the proposed rule.

For example, the NPRM solicits input on the costs and benefits of requiring aggregation across both fiat and CVC and Digital Assets with Legal Tender Status ("LTDA") transactions.[35] If adopted, such an approach would seemingly require banks and MSBs to aggregate transactions involving bank accounts (and other fiat-based accounts) and CVC wallets. As noted above, the aggregation requirement in the proposed rule will already require industry to spend significant time and money on the development of technology solutions. Requiring aggregation across CVC and LTDA transactions would serve to further compound this issue. Nor is it consistent with rules applicable to cash and other monetary instruments, which do not require aggregation with other transfers such as ACH transactions, nor include a 24-hour rolling reporting period.

Similarly, while the NPRM as currently drafted exempts wallets hosted at BSA-regulated financial institutions and foreign financial institutions, the NPRM solicits feedback on an alternative approach whereby FinCEN would "apply the reporting requirement to all CVC/LTDA transactions by hosted wallets, including those with hosted wallet counterparties."[36] Such an approach, which would require reporting on transactions occurring between hosted wallets, would serve to significantly increase the volume of reportable transactions and heighten the already significant compliance costs that would be imposed by the NPRM. It also is unlikely such an expansion would provide any material benefit to law enforcement since most hosted wallet providers already have robust KYC processes and are required to file suspicious activity reports, meaning law enforcement has significant insight into both ends of such transactions already.

The NPRM also floats the idea of requiring verification of the identity of counterparties in questions 15 and 21. Such a requirement would introduce an issue of first impression under any AML compliance regime because, under the existing BSA framework, "identity verification" applies only to "customers" of a financial institution. Such a concept would be a dramatic departure from existing regulatory requirements applicable to banks and MSBs. It is also unclear how banks and MSBs would conduct such verification as a practical matter, since those entities do not have an existing relationship with the counterparty. One member estimated that just obtaining and verifying the identity of customer counterparties would require an additional 200 hours a year and $40,000 in annual operational costs. It would also present a significant burden on consumers who may need to be verified by multiple financial institutions on a regular basis.

While we have not explored these considerations in full, given the limited time in which we have to respond, the Chamber believes the above potential changes would impose even more significant compliance challenges and are concerned to see Treasury floating such dramatic and expansive changes to the already over-broad NPRM.

V. Privacy Considerations

The Chamber also has concerns regarding the privacy risks that come with the increased aggregation, retention, and transmission of data. While the Chamber appreciates the importance of providing timely, accurate, and useful information to law enforcement, that goal must also be weighed against the importance of protecting the security and privacy of customers. Such concerns

[35] NPRM at 38351.
[36] *Id.*

are particularly acute in light of recent events, including the recent news that SVR hackers, the Foreign Intelligence Service arm of the Russian government, gained access to data of 18,000 organizations and individuals, including multiple key government agencies with law enforcement, military, and intelligence functions,[37] and the so-called FinCEN Files leak from earlier this year in which more than 2,500 sensitive documents sent from a number of financial institutions to FinCEN were leaked to the media, including over 2,000 SARs.[38] By FinCEN's own admission, the leak has the potential to impact U.S. national security, compromise investigations, and threaten the safety of institutions and individuals who file such reports.[39]

The NPRM would require a dramatic increase in the reporting of sensitive personal and financial information to FinCEN, the majority of which would not provide any clear law enforcement benefit. The required increase in the collection and reporting of sensitive information will inevitably increase the risk to consumers of hacks, data breaches, and leaks. It will similarly increase physical security concerns for CVC holders who may be subject to physical harm or threats from bad actors should their identity become known, particularly those storing CVC in self-hosted wallets.[40] While this risk might be justified if the increased reporting was likely to have significant law enforcement benefits, that is not the case here.

It is also critical to note the unprecedented scope of information FinCEN would have regarding nearly every blockchain transaction. By combining information contained in CVC transaction reports including the name, physical address, and blockchain address of the customer and the counterparty, FinCEN will be able to create a constantly updating map of who owns which public addresses on relevant blockchains and be able to track every transaction those wallet owners make, whether below or above the reporting and recordkeeping thresholds. The magnitude of this information cannot be understated – it includes not only the information related to the transaction at hand, but also every transaction that the counterparties to the transaction make both before and after that one transaction. To spell this out more clearly, this means that a counterparty to a transaction who never had an account relationship with the bank or MSB will have its entire wallet history and future transactions exposed to both that financial institution and the government. This is an extraordinary expansion of the amount of information provided to third parties about non-customers. It is also worth emphasizing that such government visibility into private financial activity is well beyond anything that exists in the fiat context.

Such a result could easily spell the end of any semblance of financial privacy for Americans using blockchain technology. The Chamber believes most Americans would view the government's

---

[37] Ellen Nakashima & Craig Timberg, *Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce,* The Washington Post (Dec. 14, 2020), https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html.

[38] *FinCEN Files: All you need to know about the documents leak*, BBC News (Sept. 21, 2020), https://www.bbc.com/news/uk-54226107.

[39] David Pegg, *Leak reveals $2tn of possibly corrupt US financial activity*, The Guardian (Sept. 20, 2020), https://www.theguardian.com/us-news/2020/sep/20/leak-reveals-2tn-of-possibly-corrupt-us-financial-activity.

[40] *See, e.g.,* Marie Huillet, *Norwegian Bitcoin Millionaire Jumps From Balcony to Flee Armed Burglar*, Coin Telegraph (Sep. 09, 2019), https://cointelegraph.com/news/norweigan-bitcoin-millionaire-jumps-from-balcony-to-flee-armed-burglar; Osato Avan-Nomayo, *Doxxed Ledger users in danger of physical harm*, Coin Telegraph (Dec. 21, 2020), https://cointelegraph.com/news/doxxed-ledger-users-in-danger-of-physical-harm.

ability to track every financial transaction they make as a shocking invasion of privacy. While there are good reasons to report certain transactions to the government, such as when suspicious activity is detected, enabling such granular tracking of individuals' financial activities surely cannot be justified. The Chamber also notes that in addition to FinCEN or other government actors, individual BSA-regulated entities (in the U.S. and elsewhere) could also create similar, albeit less complete, maps of their own.

VI. Additional Specific Problems with the NPRM

In the sections above, the Chamber has endeavored to set forth categories of deficiencies with both the process of the rulemaking itself as well as the substance of the proposed rule, despite the heavily truncated time period for response. Set forth below are additional specific examples of shortcomings, missing elements, and additional issues in need of resolution based on the text of the proposed rule. Necessarily, because of the timeframe provided for response, this list is incomplete, and many more specific problems likely exist, but there is simply not time to identify them. However, at a minimum, the Chamber notes the following specific problems and, where possible, potential solutions that our members were able to provide on very short notice, and notes again that a longer comment period would undoubtedly allow our members to provide additional and more detailed suggestions for improvement.

1. Any final rule should have a delayed compliance date.
    - Given the challenges of compliance with the NPRM as drafted, including the need to develop new technology solutions to monitor transactions (discussed above), it would be unreasonable to expect banks and MSBs to be able to comply with such a rule in the near future. Indeed, in the absence of significant de-risking and/or overreporting, achieving full compliance may be impossible for all but the most sophisticated entities with sufficient money and resources to rapidly develop and/or implement new technology and make associated changes to their compliance and customer support functions. Therefore, any final rule should not require compliance for at least six months after publication. Other significant regulatory changes such as the recently implemented CDD rule have taken years to become effective, and there is no reason to arbitrarily rush this rule into effect.

2. CVC should not be included within the scope of "monetary instruments" for purposes of Section 1010.316.
    - "Determining" CVC is within the scope of "monetary instruments" for purposes of Section 1010.316 is inaccurate and will create confusion about the status of CVC. While the NPRM states that the "proposed determination is not intended to affect the regulatory definition of 'monetary instruments' at 31 CFR 1010.100(dd), or the use of that regulatory definition elsewhere in FinCEN's regulations"[41] we believe the proposed structure will inevitably create unnecessary confusion. Such confusion is further compounded by the recent Funds Transfer/Travel Rule NPRM, which seeks to "clarify the meaning of 'money' as used in the Recordkeeping Rule and the Travel Rule …. the proposed rule would explicitly clarify that these rules apply to transactions involving (1) CVC, or (2) any digital asset having legal tender

[41] NPRM at 38346.

status."[42] Therefore, FinCEN appears to be creating a regime where CVC constitutes monetary instruments in some cases, money in other cases, and "value that substitutes for currency" in others.[43] This divergent approach promises to create a confusing and potentially contradictory CVC regulatory regime, highlights FinCEN's attempts to shoehorn CVC into existing provisions in an effort to stay within the BSA's statutory authority, and underlines that CVC is in fact distinct and any rules should accurately reflect its characteristics. The implementation of modifications to the BSA's definitions by the 2021 NDAA, made effective on January 1, 2021 by Congressional override of a Presidential veto, only underscores the need for more time to understand the implications of such changes, as well as any proposed implementations of such definitions by NPRM.

3. Any final rule should use consistent terms in the preamble and actual text of the rule.
    - The preamble of the NPRM spends considerable time discussing what it calls "unhosted" and "hosted" wallets, including defining such terms and assessing their relative impact on efforts to prevent illicit finance. However, the actual text of the proposed rule makes no reference to "unhosted" or "hosted" wallets and instead uses a roundabout mechanism of capturing all CVC transactions and then exempting transactions involving BSA-regulated entities and foreign financial institutions. Such an approach is likely to create confusion and may be fraught with unforeseeable and unintended consequences. It would also make the rule's preamble, which industry often looks to for guidance, less useful. Any final rule should take a consistent approach throughout and use the same terminology in the preamble as in the actual rule.

4. The Foreign Jurisdictions List is unnecessary and should be eliminated.
    - The Foreign Jurisdictions List proposed in the NPRM is superfluous and unnecessary. The NPRM states that the list would initially include Iran, North Korea, and Burma. Iran and North Korea are already subject to comprehensive embargoes imposed by the Office of Foreign Assets Control ("OFAC"), meaning nearly all transactions involving the two countries are prohibited. Burma is included on the Financial Action Task Force's so-called "grey list" as a jurisdiction with strategic deficiencies and therefore may already be treated as higher risk by banks and MSBs. Therefore, the inclusion of an additional FinCEN list would add little or no value as compared to existing requirements and controls.

5. Self-hosted wallets owned by a bank's or MSB's customer should be exempted from the rule.
    - FinCEN should consider creating an exemption to both the recordkeeping and reporting provisions of the NPRM for transactions involving self-hosted wallets owned by the bank's or MSB's customer. We believe the category of conduct of primary interest to law enforcement are transactions involving third parties not previously known to the bank or MSB. Banks are already required to conduct

[42] Threshold for the Requirement To Collect, Retain, and Transmit Information on Funds Transfers and Transmittals of Funds That Begin or End Outside the United States, 85 Fed. Reg. at 68016.
[43] 31 C.F.R. § 1010.100(ff)(5)(i)(A).

KYC on their customers pursuant to the CIP and CDD rules and MSBs must retain sufficient information to meet their other compliance requirements, including SAR filing and travel rule obligations, and, therefore, also typically have robust KYC procedures for their customers. Therefore, the imposition of this rule with respect to transfers involving a bank's or MSB's customer's own wallet would not provide new or additional helpful information for law enforcement in the vast majority of instances.

6. The proposed rule should explicitly incorporate a "reasonable basis" standard for determining whether a wallet is held at a BSA-regulated entity or foreign financial institution.
    - In the preamble of the NPRM, FinCEN states that "banks and MSBs would need to have a reasonable basis to determine that a counterparty wallet is a hosted wallet at either a BSA-regulated financial institution or a foreign financial institution in a jurisdiction that is not on the Foreign Jurisdictions List."[44] It then provides examples of methods for establishing a reasonable basis such as determining if an entity is registered as an MSB with FinCEN.[45] The preamble also adds that when dealing with a foreign financial institution, banks and MSBs need to "apply reasonable, risk-based, documented procedures to confirm that the foreign financial institution is complying with registration or similar requirements that apply to financial institutions in the foreign jurisdiction." However, none of this language is contained in the actual text of the rule. We believe the rule should explicitly incorporate this "reasonable basis" standard into the rule itself, especially given the disconnect in terminology used in the preamble versus the proposed rule itself. Additionally, to the degree FinCEN expects banks and MSBs to confirm the registration status of foreign financial institutions, the Chamber notes that there is presently no way for banks or MSBs to determine such registration status, as most jurisdictions do not have a publicly available database of all registered financial institutions.

7. The "prevailing exchange rate" standard should be included in the text of the actual rule.
    - The preamble to the NPRM states that the recordkeeping and reporting requirements should be based on the "prevailing exchange rate at the time of the transaction."[46] Footnote 64 of the NPRM then defines "prevailing exchange rate." However, that definition is not included in the actual text of the rule itself and the term "prevailing exchange rate" only appears in the text of the recordkeeping rule, not the reporting rule. If FinCEN intends to impose such a standard and utilize the definition contained in the preamble, that should be clearly stated in the text of the actual rule.

[44] NPRM at 83849.
[45] *Id.*
[46] NPRM at 83848.

8. The NPRM should explicitly permit banks and MSBs to obtain counterparty information from their customer and provide a safe harbor for banks and MSBs that do so.
    - While the NPRM does not address how banks and MSBs are supposed to collect counterparty information, including name and physical address, the reality is that such institutions will have to rely on their customers to provide that information. It would be unreasonable to hold banks and MSBs accountable for a customer's provision of inaccurate counterparty information. Therefore, banks and MSBs should be able to obtain counterparty information from their customers and should be permitted to rely on such information. By way of example, the Customer Due Diligence Final Rule clarified that a covered financial institution may rely on the information supplied by the legal entity customer regarding the identity of its beneficial owner or owners, provided that it has no knowledge of facts that would reasonably call into question the reliability of such information. FinCEN further explained that financial institutions would generally be able to rely on the representations of the customer as to the identities of its beneficial owners.[47] While the CDD Rule provided a standard for collecting information on beneficial owners of legal entity customers, Treasury should provide a similar - if not more deferential - standard with respect to collecting information on counterparties.

9. FinCEN should identify a standard for assessing counterparty information.
    - The NPRM states that banks and MSBs should "continue to follow risk-based procedures to determine whether to obtain additional information about their customer's counterparties or take steps to confirm the accuracy of counterparty information."[48] However, this language is only contained in the preamble to the rule and is not contained in the text of the rule itself. To the degree FinCEN intends to require banks and MSBs to implement risk-based procedures to confirm the accuracy of counterparty information, FinCEN should clearly state so in the text of the rule itself. It should also provide guidance on how it will assess whether a bank or MSB has implemented appropriate risk-based controls.

10. FinCEN should broaden the scope of exemption for dealings with other BSA-regulated entities.
    - The exemption for CVC transactions involving wallets held at other BSA-regulated entities applies to "a transaction in convertible virtual currency or a digital asset with legal tender status that is between the financial institution's customer and a counterparty whose account is held at a financial institution regulated under the BSA, or at a foreign financial institution …." By limiting the exemption to transactions involving a financial institution's customer and counterparty, the exemption does not appear to cover other types of transactions such as: (1) an MSB or bank's transfers from deposit wallet addresses to omnibus wallet addresses, (2) an MSB or bank's transfers from a hot wallet to a cold wallet or vice versa; and (3) an MSB or bank's transfers of its own CVC to another MSB. The Chamber believes that recordkeeping and reporting on such transactions would be of little law enforcement value and involve conduct on which MSBs and banks already

[47] Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. at 29415.
[48] NPRM at 83850.

create and retain internal records. Therefore, the scope of the exemption should be broadened to capture other types of conduct, such as those listed above.

11. Exemptions for existing CTR rule should be extended to CVC transactions.
    - The NPRM, at footnote 59, explicitly states that the exemptions for listed companies and their subsidiaries applicable to CTRs and contained at 31 C.F.R. § 1020.315(4)-(5) are not applicable to the proposed CVC transaction reports. The NPRM is silent on exemptions contained 31 C.F.R. § 1020.315(6)-(7). Particularly given the rise in use of stablecoins for payment purposes, many non-crypto companies are opening accounts with banks and MSBs handling CVC transactions related to day-to-day business activity such as paying business expenses or employee salaries. These exemptions, which are allowed for transactions in cash, should be similarly extended to transactions in CVC. As described elsewhere in this comment letter, law enforcement already has significantly more insight into CVC transactions than it does for cash transactions. Therefore, applying a more stringent standard to CVC transactions is without merit.

12. FinCEN should clarify that batch reporting will be allowed for CVC transaction reports as it is for CTRs.
    - The NPRM does not explicitly reference the availability of batch reporting for CVC transaction reports. The Chamber assumes that FinCEN will permit such batch reporting, as it has for CTRs, but believes its members would be reassured by explicit reference to batch reporting in any final rule or in accompanying guidance. If banks and MSBs were not permitted to report in batches, and instead were required to individually file CVC transaction reports, it would significantly increase the compliance burden imposed on such entities.

13. FinCEN should change the aggregation requirement from any "24-hour period" to a "single business day."
    - The aggregation rule in the NPRM contained at Section 1010.313 requires aggregation of certain transactions in CVC "during a 24-hour period." Notably, this is a different standard than is used for transactions in currency which is "during any one business day" (and clarifies that "[d]eposits made at night or over a weekend or holiday shall be treated as if received on the next business day following the deposit."). While unclear from the NPRM, use of the term 24-hour period suggests that banks and MSBs will need to aggregate CVC transactions on a continuous, rolling 24-hour basis. This will undoubtedly require additional technological solutions and greatly complicate compliance. Use of a standard "business day" as is used for currency would significantly reduce the compliance burden and the NPRM articulates no reason for treating CVC transactions differently from currency in this regard.

14. FinCEN should clarify that exempt transactions do not count toward the $10,000 reporting threshold under the aggregation provision.
    - The Chamber believes that transactions which are exempt from the reporting requirements (i.e. those involving a BSA-regulated entity or foreign financial

institution) would not count toward the $10,000 threshold with respect to the aggregation provision in the NPRM. However, this is not explicitly stated in the proposed rule. Any final rule should specifically state such exempt transactions should not be included in the required aggregation.

15. FinCEN should provide targeted lists of self-hosted wallets for reporting.
    - Rather than requiring blanket reporting on all transactions above $10,000 with self-hosted wallets, which will primarily generate a deluge of unhelpful information related to entirely lawful transactions, FinCEN could periodically provide industry with a targeted list of self-hosted wallets for which certain higher risk factors exist and require reporting on that subset of wallets for a specific period of time.

VII. Additional Questions

From a practical perspective, it was simply not feasible for the Chamber and its members to provide meaningful comments on all possible topics of concern in such a short period of time. Implementation of the rule would be complex, a fact implicitly acknowledged by FinCEN in the NPRM by listing 24 distinct questions on which the agency is seeking input. Implementing the NPRM will require banks and MSBs to make changes to their compliance departments, customer service teams, and IT infrastructure, among other measures. Collecting input from these various internal stakeholders is a time-consuming process and one made even more difficult given the concurrence of the comment period with the holiday season. Set forth below is a list of topics that we were not able to fully cover in this comment letter because of the condensed timetable.

Of particular note are the implementation-related questions raised by members, which highlight the difficulty and, in certain instances, impossibility of fully complying with the rule as currently drafted. In the absence of additional clarity from FinCEN regarding these important questions, industry will be left to guess at its regulatory obligations and the application of the proposed rule to various factual scenarios and business models.

1. Implications for decentralized finance, decentralized applications, and smart contracts.
    - It is unclear whether the recordkeeping and reporting provisions of the NPRM would be triggered when MSBs and banks send funds from a hosted wallet to a non-custodial smart contract. Given that these contracts have no direct owner and, in some cases, are governed by hundreds if not thousands of governance token holders, it will be impossible for an MSB or bank to comply in such situations. Another example is trade finance and smart contracts intended to mimic letters of credit or similar instruments. In such cases there is likely to be a number of persons involved in the transaction chain, one or more of whom may be unknown to the original transferor. As drafted, the NPRM could cause banks and MSBs to stop integrating these types of protocols into their product offerings, which would dramatically impair innovation and competitiveness. This would not only hurt banks and MSBs, but would harm individual consumers by limiting their access to new and innovative financial services and products and creating friction for transfers between decentralized finance projects and banks and MSBs.

2. Implications for the use of Layer 2 Protocols.
    - The NPRM does not address how banks and MSBs should handle transactions involving "layer 2" solutions such as the Lightning Network, which use off-chain micropayment channels. The Lightning Network allows counterparties to engage in multiple off-chain transactions, which are only recorded to the blockchain when the counterparties open and close a channel. How such layer 2 transactions should be recorded and reported is not addressed in the NPRM, leaving industry to guess at how FinCEN intends the proposed rule to be implemented in such contexts.

3. Implications for Digital Assets with Legal Tender Status if such assets gain significant traction.
    - The implications of this rule for LTDA are potentially immense. Given the condensed timetable to respond and that such assets are not currently in wide use, the Chamber has not focused its letter on this topic. However, we wish to briefly note the potentially significant implications of the inclusion of LTDA in this NPRM. For example, if interpreted broadly, this concept could potentially capture central bank digital currencies issued by any country, including potentially a digital dollar issued by the Federal Reserve. This would lead to an overwhelming volume of records and reports and a stunning invasion of personal privacy. Given the 12-day/6 business day comment period, a full exploration of these issues is simply not possible, but the potential impact is dramatic and clearly requires further consideration by industry and government.

4. Determining thresholds when handling newly minted or illiquid CVC with no established markets for determining the price of such assets in dollars.
    - In many cases it will be relatively easy to determine the price of CVC in dollars. This is particularly true for widely used CVC such as bitcoin or ether with well-established liquid markets for dollar conversion. However, this is not the case for less liquid or newly issued digital assets. For such assets, the prices may vary significantly between exchanges or there may be no established dollar price at all. Similar concerns also exist in the over-the-counter context where the price of a given transaction may differ from prices offered in public markets.

5. Determining whether a given digital asset constitutes CVC.
    - The NPRM defines CVC as "a medium of exchange (such as cryptocurrency) that either has an equivalent value as currency, or acts as a substitute for currency, but lacks legal tender status." This is a broad and amorphous definition that, without more detailed guidance, will leave banks and MSBs with significant uncertainty over the status of many assets and lead to additional over-reporting. Further, we noted in our response to the travel rule NPRM that the phrase "(such as cryptocurrency)" be removed from the definition as it introduces another undefined term.[49]

[49] Letter from The Chamber of Digital Commerce, to Ann E. Misback, Sec'y of the Bd. Of Governors of the Fed. Res. Sys. (Nov. 25, 2020), at 8, https://4actl02jlq5u2o7ouq1ymaad-wpengine.netdna-ssl.com/wp-content/uploads/2020/11/Chamber-of-Digital-Commerce-Response-to-FinCEN-Travel-Rule-NPRM-112520.pdf.

6. Treatment of multi-signature wallets.
    - The NPRM does not address the treatment of multi-signature ("multi-sig") wallets. FinCEN has previously issued guidance on multi-sig wallets and whether such wallets should be considered hosted or self-hosted,[50] and the Chamber believes such guidance should remain applicable in the context of this proposed rule. However, that is not clear from the NPRM itself.

7. Impact on financial inclusion.
    - The Chamber believes the NPRM's impact on financial inclusion could be enormous and should be specifically considered and addressed by FinCEN before implementing a final rule. Millions of Americans are either unbanked or underbanked and access to financial services has only become more difficult during the current COVID-19 pandemic. Unfortunately, regulatory changes have all too often exacerbated rather than ameliorated the problem of financial inclusion. The Chamber also notes that the issue of financial inclusion is closely tied to fighting illicit finance, as individuals who are excluded from the regulated financial sector are likely to turn to unregulated or offshore providers or to engage in direct peer-to-peer transactions with no financial institution involvement.

8. Constitutionality of the significant invasion of privacy that would be facilitated by the NPRM.
    - As noted above, the NPRM would allow FinCEN, and potentially other U.S. government agencies, to create maps of relevant blockchains tying an individual's name and address to public wallet addresses and tracking every transaction such persons make for so long as a person holds a given address for lawful transactions. This would provide the government with an unprecedent level of surveillance over individual American users and spell an end to financial privacy for many, perhaps most, blockchain users. We believe that such an expansion clearly implicates the Fourth Amendment rights of surveilled Americans and that FinCEN must either provide a clear and detailed explanation of the constitutionality of the NPRM or commit to the implementation of safeguards to prevent the aggregation and misuse of reported data. The Chamber has deep concerns regarding these matters, which it believes must be addressed before the issuance of a final rule.

9. Timing requirement for receipt of CVC.
    - The NPRM states "in the case of a transaction in which the bank's or MSB's customer is the recipient, the bank or MSB would need to obtain the required recordkeeping and verification information as soon as practicable."[51] The "as soon as practicable" standard is contained only in the NPRM's preamble and not in the actual text of the proposed rule. If FinCEN intends to use such a standard going forward, it should be clearly stated within the text of the actual rule. In addition, while this language seemingly reflects the reality that a bank or MSB may not have

[50] FinCEN, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (May 9, 2019), at Section 4.2, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.
[51] NPRM at 83849.

advance notice of CVC being transmitted to a wallet within its control, it raises a number of other questions. Will banks or MSBs be penalized if they are unable to obtain the information in a given period of time for reasons outside their control? Will banks or MSBs be penalized if their customer declines to provide the necessary verification or counterparty information? Should a bank or MSB file a SAR in all such instances?

10. Lack of transactional-related definitions in the NPRM.
    - The NPRM requires customer verification prior to "concluding" a transaction in CVC/LTDA. However, the NPRM does not define the term "concluding" nor does it define the term "transaction." This lack of definition leaves open a number of questions. How does FinCEN define the conclusion of a blockchain transaction? Is the relevant transaction the crediting or debiting of a customer's account or is it the underlying transaction confirmed on the blockchain itself?

11. Ambiguity in aggregation requirement.
    - The requirement to aggregate CVC/LTDA transactions in the NPRM is vague in a number of respects. The NPRM requires aggregation when the bank or MSB has knowledge that transactions by or on behalf of any person "result in value in or value out of convertible virtual currency or digital assets with legal tender status with a value of more than $10,000 during a 24-hour period." However, it is not clear if value in and value out transactions should be aggregated together or if they should be calculated separately for purposes of the $10,000 threshold.

12. Ambiguity regarding transactions with multiple senders or recipients.
    - The preamble to the proposed rule notes, "… CVC/LTDA transactions may involve multiple senders and recipients …. a transaction where any one participating wallet is unhosted or otherwise covered would be subject to the proposed CVC/LTDA transaction reporting requirement …. banks and MSBs would be required to report, keep records, and engage in verification with respect to such transactions, if the aggregate amount of CVC/LTDA … exceeds $10,000 in value within a 24-hour period."[52] However, the NPRM provides no guidance with regard to handling such transactions. Who should be treated as a customer? Who should be treated as a counterparty? How should such information be reported? Will the reporting system allow for input of multiple recipients and senders? How should intermediary persons (*i.e.*, not senders or recipients) be treated? All of this must be clarified in any final rule or industry will be placed in an impossible position of attempting to resolves these questions itself.

13. Ambiguity regarding transaction hashes.
    - The NPRM states "the proposed rule would cause banks and MSBs to generate reports containing the transaction hash and identity of persons holding wallets engaging with unhosted or otherwise covered wallets engaging in transactions across multiple financial institutions."[53] However, the text of the proposed rule

[52] *Id.*
[53] NPRM at 83845.

itself contains no reference to reporting a "transaction hash." The recordkeeping rule includes the very broad requirement of "any other information that uniquely identifies the transaction," but similar language is not contained in the reporting requirement text. Any specific obligations with respect to the transaction hash must be more clearly stated in the actual text of the rule.

14. Impact on other governmental agencies.
    - A variety of other governmental agencies rely upon FinCEN regulations when engaged in their own rulemakings, publication of guidance, and enforcement actions. For example, the Internal Revenue Service, FinCEN's delegated examiner for MSBs, and the federal functional regulators that oversee other types of financial institutions, are tasked with interpreting and applying FinCEN regulations when conducting BSA examinations and considering enforcement activity. Similarly, many state banking and financial regulators look to FinCEN regulations for guidance in creating state-level rules, such as the application of state money transmitter licensing regimes to dealings in CVC. If FinCEN's rules are vague or internally inconsistent, it will inevitably lead to confusion among other governmental agencies and lead to divergent approaches taken by such agencies, which may make compliance difficult or impossible for industry. Such an outcome will also be problematic for FinCEN, which will ultimately be called upon to help resolve these differing approaches.

The Chamber believes that, in the absence of additional clarity on a number of the above questions, it will be difficult or impossible for industry to implement the rule in an appropriate manner, absent significant de-risking and/or overreporting. The vague and confusing provisions cited above must be remedied before issuing a final rule.

In addition to the above questions, the Chamber was not able to address a number of questions specifically posed by FinCEN in the NPRM, including:

- (5) Describe how the costs of complying with the proposed reporting requirement, or the benefits to law enforcement from the data obtained from the proposed reporting requirement, would vary were FinCEN to adopt a higher or lower threshold than $10,000.

- (7) Should FinCEN add additional jurisdictions to the Foreign Jurisdictions List or remove jurisdictions currently on that list? Are there any particular considerations FinCEN should take into account when adding or removing jurisdictions?

- (10) Has FinCEN properly considered the extension of the mandatory and discretionary statutory exemptions at 31 U.S.C. 5313(d)-(e) that are currently applicable to the CTR reporting requirement to the proposed CVC/LTDA transaction reporting requirement? Has FinCEN extended exemptions either too broadly or too narrowly? Was FinCEN correct to not extend the exemption from the CTR reporting requirement at 31 CFR 1010.315 related to transactions between a non-bank financial institution and a commercial bank to the proposed CVC/LTDA transaction reporting requirement?

- (11) Should FinCEN extend the obligation to file reports under the proposed CVC/LTDA transaction reporting requirement to financial institutions other than banks and MSBs (e.g., brokers-dealers, futures commission merchants, mutual funds, etc.)? What would be the cost and benefits of extending the proposed CVC/LTDA transaction reporting requirements to other financial institutions?

- (14) Could the verification requirements be adjusted to enhance the benefits to law enforcement without a significant change to the costs to banks and MSBs, or to reduce the costs to banks and MSBs without a significant change in the benefit to law enforcement?

- (16) Is it necessary for the anti-structuring prohibition to be extended to the proposed CVC/LTDA transaction reporting requirement?

- (17) Would it be appropriate for FinCEN to require additional data be retained pursuant to 31 CFR 1010.410(g)?

- (20) Could the verification requirements be adjusted to enhance the benefits to law enforcement without a significant change to the costs to banks and MSBs, or to reduce the costs to banks and MSBs without a significant change in the benefit to law enforcement?

- (22) Is it reasonable to require that records be retained in electronic form? Are the retrievability criteria reasonable?

- (23) Should FinCEN extend the obligation to keep records under the proposed CVC/LTDA transaction reporting requirement to financial institutions other than banks and MSBs (e.g., broker-dealers, futures commission merchants, mutual funds, etc.)?

These are important questions in their own right, and the inability of the Chamber to address these within the timeframe given (as well as the scope and breadth of issues identified in this letter) is simply further proof that the timeframe for response to this NPRM is simply inadequate.

VIII. Conclusion

The Chamber stands ready to work with FinCEN to meet the important regulatory challenges relating to self-hosted wallets, but the process must be adequate to this important task. FinCEN should allow the full participation of the public and affected parties and to tailor any final rule in a way that will actually produce helpful information for law enforcement and do so in a manner that will not impose significant cost on industry. The Chamber again requests a 90-day extension of the comment period to permit it to fully address the more than two dozen issues raised for public comment by FinCEN. We also believe that, given the expansive list of open questions as well as constructive feedback offered in this letter, FinCEN should issue another NPRM to address its proposed solutions. Should FinCEN nevertheless decide to move forward, it should consider implementing the recommendations provided by the Chamber above. And the final rule should provide a full 30-day effective period as required by the APA and a deferred compliance date that will allow the industry to prepare for these new, costly, and technologically challenging regulatory requirements.

Very Truly Yours,

Amy Davine Kim
Chief Policy Officer

cc: Jason Weinstein
Alan Cohn
Shannen Coffin
Evan Abrams
Steptoe & Johnson LLP

Attachment A – Chamber Letter to Secretary Mnuchin

CHAMBER OF DIGITAL COMMERCE

December 22, 2020

The Honorable Steven T. Mnuchin
Secretary of the Treasury
U.S. Department of the Treasury
1500 Pennsylvania Avenue, NW
Washington, DC 20220-0002

Re: Request for Extension of Time: FinCEN Docket Number FINCEN-2020-0020; RIN 1506-AB47; Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets

Dear Secretary Mnuchin:

The Chamber of Digital Commerce (the "Chamber")[1] writes this letter with respect to the Financial Crimes Enforcement Network ("FinCEN") Notice of Proposed Rulemaking related to the "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets" (the "NPRM"), to request that you extend the comment period by 90 days to allow for full participation of affected parties and to better permit FinCEN to gauge the impact and any concerns with the proposed rule. Absent this extension, the proposed rule risks lacking legitimacy under the Administrative Procedure Act ("APA").

The proposed rule, which has yet to be published in the Federal Register, provides only 15 days for affected parties to provide comment. Those fifteen days, which fall over the Christmas and New Year's federal holidays as well as two weekends, provide a mere 8 business days to comment. This truncated time frame makes it impossible to fully evaluate the effect of the rule, identify any problems of compliance and unforeseen

[1] The Chamber is the world's largest blockchain trade association. Our mission is to promote the acceptance and use of digital assets and blockchain technology, and we are supported by a diverse membership that represents the blockchain industry globally. Through education, advocacy, and close coordination with policymakers, regulatory agencies, and industry across various jurisdictions, our goal is to develop a pro-growth legal environment that fosters innovation, job creation, and investment. We represent the world's leading innovators, operators, and investors in the blockchain ecosystem, including leading edge startups, software companies, global IT consultancies, financial institutions, insurance companies, law firms, and investment firms. Consequently, the Chamber and its members have a significant interest in blockchain and distributed ledger technology.

consequences of the proposed regulation, and decide how to respond to two dozen questions raised for public comment.

Given the significant impact of the proposed rule, the 15-day comment period is wholly inadequate and raises serious process concerns under the APA. Having subjected the rule to notice and comment procedures, the agency has an obligation not to act in arbitrary or capricious manner. Courts have interpreted the APA to provide that an "exceedingly short" comment period does not "provide a meaningful opportunity for comment." *N. Carolina Growers' Ass'n, Inc. v. United Farm Workers*, 702 F.3d 755, 770 (4th Cir. 2012).

Only "rare" instances "actually warranting" a shortened comment period will a comment period as short as this one be permitted. Those rare situations "are generally characterized by the presence of exigent circumstances in which agency action was required in a mere matter of days." *Id.* The need to rush this rule out before the expiration of this Administration is not one of them. Courts regularly conclude that an "emergency of the [government's] own making" does not constitute good cause. *NRDC v. Abraham*, 355 F.3d 179, 205 (2d Cir. 2004); *see also Levesque v. Block*, 723 F.2d 175, 184 (1st Cir.1983) (concluding imminence of self-imposed deadline did not qualify as good cause to dispense with notice-and-comment before issuing final rule).

Nor do we believe that the agency could, as it claims, satisfy the "good cause" standard or foreign affairs function exceptions to dispense with notice and comment procedures. Indeed, by providing notice and comment (albeit insufficient notice and comment), the NPRM undermines its own claims that these exceptions are applicable, as they generally relate to the impracticability of notice and comment and/or harm to foreign affairs or the public interest that might stem from providing public notice and comment. In any event, the national security exigencies identified in the NPRM are not sufficient to dispense with an adequate period for comment. For instance, the risk of malign actors taking action to circumvent the rule, assuming it exists, arose the moment the agency decided to go the NPRM route—it is not substantially increased by permitting a longer comment period, since the transactions that the agency fears will occur take mere minutes, not weeks, to complete. Nor is there reason to believe that bad actors utilizing banks and money services businesses in light of existing regulatory requirements, such as the reporting of suspicious activity, will be so alarmed by the publication of this NPRM as to flee such platforms in mass, and, indeed, none of our members have reported any such exodus of funds or users. A longer comment period may allow the agency to better calibrate its rule to reduce such risks in the future.

These are significant risks to the legitimacy of the proposed rule within the current truncated process. An extension to provide a fuller study of the proposed rule and its implications is not only consistent with prior practice in similar FinCEN rules, but also will allow us to work cooperatively with FinCEN to meet law enforcement objectives while serving to allow this industry to grow responsibly.

We thank you for your consideration.

Very truly yours,

Perianne Boring
Founder and President

Amy Davine Kim
Chief Policy Officer